## REMARKS

The Examiner rejected claims 5-7, 10-12 and 19-30 under 35 U.S.C. §112, second paragraph.

The Examiner rejected claims 5, 10 and 19-30 under 35 U.S.C. §103(a) as allegedly being unpatentable over Vaidya (US Patent Number 6,279,113) in view of Sharma et al. (US Patent Number 6,909,692) hereinafter referred to as Sharma.

The Examiner rejected claims 6 and 11 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Lunt (Detecting Intruders in Computer Systems).

The Examiner rejected claims 7 and 12 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Martin et al. (US 6,772,349) hereinafter referred to as Martin.

Applicants respectfully traverse the §112 and §103 rejections with the following arguments.

09/966,227                                    7

## 35 U.S.C. §112, Second Paragraph

The Examiner rejected claims 5-7, 10-12 and 19-30 under 35 U.S.C. §112, second paragraph, as being indefinite for allegedly failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner argues: "Claims 5 and 10 recite the limitation "said denial of service attack" in line 4. There is insufficient antecedent basis for this limitation in the claim. The examiner will assume the limitation was meant to refer to the "denial of service intrusion"."

In response, Applicants agree with the preceding interpretation by the Examiner and have therefore amended claims 5 and 10 to replace "attack": with "intrusion".

Accordingly, Applicants respectfully request that the rejection of claims 5-7, 10-12 and 19-30 under 35 U.S.C. §112, second paragraph be withdrawn.

09/966,227                                        8

## 35 U.S.C. §103(a)

The Examiner rejected claims 5, 10 and 19-30 under 35 U.S.C. §103(a) as allegedly being unpatentable over Vaidya (US Patent Number 6,279,113) and further in view of Sharma et al. (US Patent Number 6,909,692) hereinafter referred to as Sharma.

Applicants respectfully contend that claims 5 and 10 are not unpatentable over Vaidya in view of Sharma, because Vaidya in view of Sharma does not teach or suggest each and every feature of claims 5 and 10.

As a first example of why , Vaidya in view of Sharma does not teach or suggest the feature: "**when the value of the signature event counter exceeds the signature threshold quantity**, generating an alert by an intrusion detection sensor of the intrusion detection system, recording a time of generating the alert in a log of a governor comprised by the intrusion detection sensor, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold" (emphasis added).

The Examiner argues that Sharma teaches "recording a time of generating the alert in a log of a governor comprised by the intrusion detection sensor, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold".

In response, Applicants agree with the Examiner that Sharma teaches "recording a time of generating the alert in a log of a governor comprised by the intrusion detection sensor,

09/966,227                                          9

determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold".

However, claims 5 and 10 require performance of:

"generating an alert by an intrusion detection sensor of the intrusion detection system"

AND

"recording a time of generating the alert in a log of a governor comprised by the intrusion detection sensor, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold"

WHEN

"the value of the signature event counter exceeds the signature threshold quantity".


Thus, claims 5 and 10 require that when "generating an alert" occurs, the "recording", "determining", and "comparing" steps also occur, because all of the preceding step are initiated WHEN "the value of the signature event counter exceeds the signature threshold quantity". Therefore, whenever "generating an alert" is performed, the "recording", "determining", and "comparing" steps are also performed.

Applicants acknowledge that Sharma teaches performing the "recording" step whenever the step of "generating an alert" is performed". However, Sharma does not teach performing the "determining" and "comparing" steps whenever the step of "generating an alert" is performed". To the contrary, Sharma, col. 9, lines 16-20 teaches that the "determining" and "comparing" steps are performed only after the step of "generating an alert" is performed" approximately 1000 times.

09/966,227            10

The preceding limitation of claims 5 and 10 are illustrated in FIG. 4 of the present patent application, which shows the "generating", "recording", "determining", and "comparing" steps 415, 420, 440, and 450, respectively, all occurring in each iteration of the loop triggered by the "Threshold Exceeded"decision step.

Accordingly, claims 5 and 10 are not unpatentable over Vaidya in view of Sharma.

As a second example of why, Vaidya in view of Sharma does not teach or suggest the feature: "when the present alert generation rate exceeds the alert generation rate threshold, altering an element of a signature set of the intrusion detection system to decrease an alert generation rate of the intrusion detection sensor" (emphasis added).

The Examiner argue that teaches the preceding feature of claims 5 and 10.

In response, Applicants acknowledge that Sharma teaches" when the present alert generation rate exceeds the alert generation rate threshold, decreasing an alert generation rate. However, Sharma does not teach decreasing an alert generation rate by the technique of "altering an element of a signature set of the intrusion detection system". And neither does Vaidya.

Accordingly, claims 5 and 10 are not unpatentable over Vaidya in view of Sharma.

Based on the preceding arguments, Applicants respectfully maintain that claim 5 is not unpatentable over Vaidya in view of Sharma, and that claim 5 is in condition for allowance. Since claims 19-24 depend from claim 5, Applicants contend that claims 19-24 are likewise in condition for allowance. Since claims 25-30 depend from claim 10, Applicants contend that claims 25-30 are likewise in condition for allowance.

09/966,227                                        11

The Examiner rejected claims 6 and 11 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Lunt (Detecting Intruders in Computer Systems).

Since claims 6 and 11 respectively depend from claims 5 and 10, which Applicants have argued *supra* to not be unpatentable over Vaidya in view of Sharma under 35 U.S.C. §103(a), Applicants maintain that claims 6 and 11 are likewise not unpatentable over Vaidya in view of Sharma and further in view of Lunt under 35 U.S.C. §103(a).


The Examiner rejected claims 7 and 12 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Martin *et al.* (US 6,772,349) hereinafter referred to as Martin.

Since claims 7 and 12 respectively depend from claims 5 and 10, which Applicants have argued *supra* to not be unpatentable over Vaidya in view of Sharma under 35 U.S.C. §103(a), Applicants maintain that claims 7 and 12 are likewise not unpatentable over Vaidya in view of Sharma and further in view of Martin under 35 U.S.C. §103(a).

09/066,227                                    12

## CONCLUSION

Based on the preceding arguments, Applicants respectfully believe that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicants invites the Examiner to contact Applicants' representative at the telephone number listed below. The Director is hereby authorized to charge and/or credit Deposit Account No. 09-0457.


Date: _04/11/2006_

_Jack P. Friedman_
Jack P. Friedman
Registration No. 44,688

Schmeiser, Olsen & Watts
22 Century Hill Drive, Suite 302
Latham, New York 12110
(518) 220-1850

09/966,227                                     13